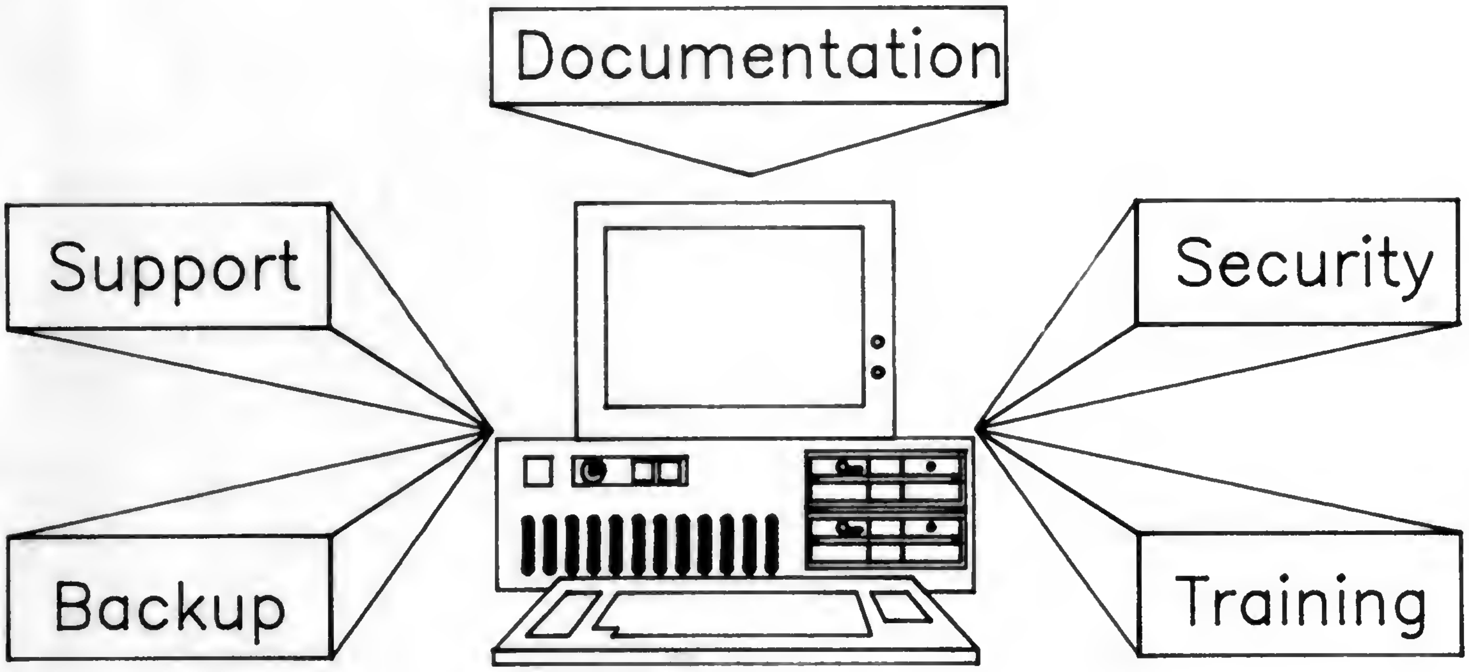
STATE OF MONTANA MICROCOMPUTER MANAGEMENT GUIDELINES



Published by:

Department of Administration
Information Services Division
Information Center Bureau

July, 1988

TABLE OF CONTENTS

MICROCOMPUTER MANAGEMENT GUIDELINES

INTRODUCTION

This guide presents some of the key questions to consider in establishing agency guidelines for the microcomputer environment. The questions should provide a framework for creating a protection program for microcomputers. The guide is intended to provide ideas for documentation, security, backup and recovery, support, training and maintenance of PC applications.

Call the Information Center at 444-2973 if you need more assistance.

DOCUMENTATION

Why do PC applications need to be documented?

Many of the application programs that run on microcomputers (in state government) are crucial to business or decision-making activities. To properly implement a PC application requires good documentation.

Good documentation takes time, costs money, and goes relatively unnoticed because it is taken for granted. Poor documentation, on the other hand, ultimately takes more time, costs more money, and is conspicuous by its absence. Documentation is not for ourselves, it is to help others. If a primary user leaves the agency or is ill for an extended period of time, a lack of good documentation will result in many long hours for the new user to understand how things work. Or even worse, for them to think they understand how things work. Good documentation also provides a consistent reference source for all members of a department -- especially newer ones.

Which PC applications need to be documented?

Each agency should develop a documentation policy which identifies the types of applications which should be documented. Applications that contribute substantially to an organization and would represent a major loss of information or affect decision making should be documented. Documentation for personal or one-time applications can be optional. As a general rule, any applications done on a regular basis should be documented. A primary and a back-up person should be specified for each application so that questions concerning the application can be answered and documentation kept current.

When I write documentation, who is the intended audience?

There are two types of documentation -- technical and user. Technical documentation is developed for the person responsible for maintaining the application. User documentation is developed for the person responsible for using the application.

As a general rule, documentation that is built-in to the application should serve as a complete guide for the application user. Built-in documentation might include such things as input and output instructions, who to contact with questions concerning the application, etc.

Technical documentation (usually external to the application) should serve as a complete guide for the support personnel. Technical documentation might include such things as file descriptions, report layouts, and spreadsheet formulas.

Where can I get help?

Software packages are available to ease the documentation chore including diskette management packages and spreadsheet documentation programs. The Information Center Bureau currently offers a class on Spreadsheet Design and Documentation and Database Concepts and Design. Many of the same techniques that apply to mainframe application design and documentation can be applied to PC's. A good reference book is How to Write Computer Documentation for Users by Susan J. Grimm.

What should proper documentation include?

Documentation procedures should be straightforward and easy to accomplish. Checklists and fill-in-the-blank documentation sheets are easiest. A sample checklist is included in Appendix A. Also see MOM 1-0232.00.

The chart in Appendix B gives an example of the information you will want to include in your documentation. Also, for more detailed information refer to the Documentation Table on page 3.

Documentation may vary depending on the type of application. There are three types of applications -- critical, organizational support, and personal or one-time.

Critical Applications-directly affect the ability to carry out the mission of the organization and for which there is no other

source of information. It is recommended that all documentation listed in the table below should be used when documenting critical applications.

Organizational Support Applications-contribute substantially to an organization and would represent a major loss of information. These applications also affect decision-making or are difficult to rebuild. The extent of documentation for these applications is up to management discretion and could include any or all of the items listed in the Documentation Table below. The decision as to what to document should include consideration of the importance and the cost of recovering the information.

Personal or One-Time Applications-are personal in nature or will only be used one time. They help a person do a better job, but are not necessary to the business without that person. Documentation is not required for this type of an application. However, we recommend at least a statement explaining what the application does and who to contact with questions or problems be built into the application.

DOCUMENTATION TABLE

There are 4 main PC application categories--Spreadsheet, Wordprocessing, Database, and Graphics. Listed below are detailed examples of technical and user documentation for each PC Application. For a quick summary of the documentation needed, see Appendix B.

SPREADSHEET

TECHNICAL	USER
Spreadsheet Map	Spreadsheet documentation (what the spreadsheet is and what it does, who to contact with questions)
Spreadsheet documentation (What the spreadsheet is and what it does; how to enter the input data; does the spreadsheet depend on other spreadsheets for its input; is this spreadsheet part of a larger application)	Printout of data entry screen, noting where data will be entered

Spreadsheet Macros should be documented	Input instructions
A sample printout of the entire spreadsheet	Output instructions
Keying instructions	Error messages (where to find explanations of them, who to contact, etc.)
Technical support info. (naming conventions, directory structure, batch files, etc.)	Backup procedures (what, how often)
Backup procedures (which files, frequency of backups, new cycle instructions)	Security procedures (what level of security is needed, what is secured, how it is to be secured)

WORDPROCESSING

TECHNICAL	USER
Description of file (what it is, what it does)	Description of file (what it is, what it does, who to contact with questions)
If macros are used, document macro names, what each macro does, and when to invoke the macro)	Macro names, description, and when to invoke
If a merge is involved, list primary and secondary file names and when to start the merge)	Merging instructions, if any
Printout of a sample final document	Error messages (where to look them up, who to contact, etc.)
Technical support information (naming conventions, directory structure, batch files, etc.)	Backup procedures (what, how often)
Backup procedures (which files, frequency, new cycle instructions)	Security procedures (what level of security is needed, what is secured, how it is to be secured)

DATABASE

TECHNICAL

Data flow diagram of the database showing the files, data entry screens, and reports generated.

Description or printout of each field of each file detailing the field type, size, and key fields.

Description of data entry screens and the fields affected.

Description of the reports generated and the fields used to get the data for the report. Also any formulas or lookups used in the report.

Documented listing of macros and/or programs used to support the database application.

Database structural diagram showing the relationships between files.

Technical support information (naming conventions, directory structure, batch files, etc.)

Backup procedures (which files, frequency, new cycle instructions)

USER

Explanation of the structure and use of the database as it appears to the user. Also the name of a contact person to answer questions.

Representation of each data entry screen and an explanation of its use.

Representation of each report that is generated and an explanation of what it means and when it is generated.

Error messages (where to find explanations, who to contact, etc.)

Backup procedures(what, how often)

Security procedures (what level of security is needed, what is secured, how it is to be secured)

Processing schedules

If password protection and limited access is an important security item, then any documentation that might give an insight as to how to circumvent the security must be protected with the same level of security as the database.

GRAPHICS

TECHNICAL

File Description of both the plot and data file (what it is, what it does)

Data overlay instructions (where data comes from, data ranges, named ranges, type of import, destination of file)

Printout of graph (label printout with font sizes, typestyles, angle, fill type, line width of objects, line style, color (edge and inside), edge width, default settings)

Plot options (device, paper to draw on, & speed to draw at, horizontal or vertical, output port, baud rate, parity)

Technical support information (naming conventions, directory where files and symbols are stored, batch files, etc.)

USER

File Description (file name, what it does, who to contact with questions)

Data overlay instructions (same as for technical)

Plot options (same as for technical)

Error messages (where to look them up, who to contact, etc.)

Backup procedures (what, how often)

Security procedures (what level of security is needed, what is secured, how it is to be secured)

What should be done when a change needs to be made to an application?

All correspondence directly related to the change should be documented. Before making a change, make sure you have a current backup first! A description of the change made to the system, the reason for the change, and a user authorized change request should be included in the documentation. Documentation for changes made to critical support applications should be based on the amount of effort required to run without the system and data or to recreate them. No documentation is needed for changes made to personal applications. A sample change request is included in Appendix C.

All system changes should be tested and supported by adequate documentation. In emergency situations, it may be necessary to make modifications without adhering to standard procedures. In these cases, documentation should be done on an after-the-fact basis. Documentation should include approvals, explanations of changes made, and testing of the modifications.

COPYRIGHT LAWS

What does it mean when software is copyrighted?

The State of Montana and your agency are liable for infringement of software copyright laws. It is the responsibility of each agency to ensure that proprietary software copyright laws are not violated as a result of an agency's use of that software. (MOM Policy on Automated Systems, Chapter 1-0200, Section 1-0232.20)

Under the U.S. Copyright Law, civil damages for illegally copied software can be $50,000 or more, depending on the amount of loss to the publisher. Failure of employees to follow licensing agreements may subject the State of Montana to potential lawsuits. It is also likely that an individual is personally liable for duplicating software.

Most software is licensed for use on one machine at a time and can be copied for the purpose of backup only. Check your software manual to ensure you do not violate your software agreement.

License agreements for all software shall be adhered to. Reproducing computer software without authorization violates copyright laws and constitutes a Federal offense. Shareware may be distributed in accordance with individual copyright agreements. Public domain software is not subject to any restrictions on copying or distribution.

Who has ownership rights of software developed by agency personnel or contracted consultants?

Without clear ownership policies in existence, agencies are placing themselves at risk. Employees terminating employment may take an application they have developed; causing short or even long term interruptions in daily operations. Policies should exist which stipulate all software developed by agency personnel or by contract personnel is state property.

COMPUTER USAGE POLICY

Why do I need a computer usage policy?

It is important to know how often a micro is being used, who is using it, and most importantly what it is being used for. Policies and guidelines should be written regarding procedures each employee is expected to observe and follow when working with microcomputers.

In some areas, a reservation log may be necessary to avoid conflicts concerning the use of a micro.

SECURITY AND RECOVERY

Who's responsible for security?

Because microcomputer resources and information are distributed throughout the organization, each agency is responsible for security of their hardware, software and data, except where the computer is part of an ISD or interagency network, then it is a joint responsibility to develop security procedures. This does not mean the agency is "on his own" when it comes to a security question or problem. For assistance, check with your agency's Security Officer or call the ISD Security Officer at 444-2829.

From whom should your PC be secured?

If most personal computers in your organization are used only to raise employee productivity, the best security measures are those administered with a light touch. However, when micros store sensitive data, security becomes critical.

An agency should have a policy about the use employees are to make of organizational resources and the behavior expected of employees. Such a policy should be so designed and implemented that it holds the employees clearly accountable for their actions.

How can information be secured from intentional/unintenional alteration?

Do not leave hardware, software and data in vulnerable places. Lock desks, doors, and windows when systems are unattended. (MOM Policy on Automated Systems, Chapter 1-0200, Section 1-0250.10)

To prevent unauthorized access, all diskettes or hard disks containing important information should be under the custody of an appropriate supervisor. An access list of employees and the data they have access to should also be maintained by the supervisor.

Backup copies of software should be stored in a secure location (locked file cabinet, fire-proof vault, etc.). Make sure this area is away from magnetic fields that may cause damage to floppy disks.

Simply locking up your computer and data will not suffice if you're part of a network or use electronic mail or a bulletin board. In these cases, additional security measures may be needed. Of these, the most common is the password. Commit your password to memory. Don't keep it next to your computer or taped to your wall. Use a unique password-numbers or letters that have no pattern and are at least 4 characters in length. Change your password every 90 days.

Data recorded on a floppy diskette is usually protected from disclosure by removing the disk from the computer and storing it in a safe place. Data stored on diskette may be protected from modification and destruction by the preparation of backup copies or by placing a write protect tab on the notch of the diskette. Security software packages for both hard and floppy disks provide such features as login and passwords, software encryption, copy protection, audit trails, etc. These features help prevent modification and destruction.

What tools and procedures are available to help make the information more secure?

Physical security of hardware and software is a start. Many devices are available to lock hardware in place and/or activate an alarm in case of removal. Also some programs require a password to gain access. Passwords should be chosen carefully and disclosed only to selected personnel. File and telecommunications encryption should be considered for certain critical information. Port protection devices limit outside access to preauthorized phone numbers. A call-back program that operates when a computer is accessed by modem is one example. For more information, call the Information Center at 444-2974 or ISD's security officer (Jack Slevin) at 444-2829.

BACKUP AND RECOVERY

What are backup and recovery procedures, and why do I need them?

With critical applications and organizational support placed on PC's, backup and recovery procedures become a requirement. Agencies should determine which information needs to be backed up, and establish procedures that will recover as much data as possible.

The general goal of backup and recovery procedures is to ensure that adequate information exists to restore the information in a microcomputer environment in the event of a machine malfunction or damage to programs or data. All microcomputer files and software packages should be backed up and all backups stored in a secure location away from the primary use area.

How often should I do a backup?

The application data needs to be backed up regularly. In most environments certain days or times are set aside to run certain applications. In many instances this may be a logical time to backup. The importance of a backup procedure is critical. A good rule of thumb in determining when to backup is to ask yourself the question, "Is it easier to backup or re-enter the information?". If a large file had to be re-entered, it could be very costly to the organization. If the software allows, original program disks should be backed up prior to their first use.

Maintain at least two backup copies of software and data. Identify sensitive or critical data files and store backup copies off-site. Establish a backup schedule and make sure it

is followed. For example, on Monday you might do a complete backup of your hard disk. On Tuesday through Friday, you should do daily backups of the data that you have modified. The most recent backup should be stored in a secure area on-site with the previous backup stored in a secure area off-site. These backups should be rotated. Check to make sure backup copies are current (MOM Policy on Automated Systems, Chapter 1-0200, Section 1-0240.10). Off-site storage is available from ISD's Record's Management Section. Call 444-2716 for more information.

What is disaster recovery?

Each agency should have a disaster recovery plan. This plan is a formalized set of procedures and actions taken to minimize agency losses due to an interruption in service. The major objective in disaster recovery planning is the timely recovery of processing for critical applications. In case of a disaster, agencies could use other agencies' equipment or they could obtain equipment from the ISD equipment pool. The following items should be considered when developing such a plan:

- Identify important applications
- Determine program/data requirements (software needed)
- Develop emergency operating schedule (what hours can you use other agencies' equipment)
- Determine resource requirements (CPU, disks, supplies, personnel)
- Select alternate processing services (hardware, software, data files)
- Establish an off-site storage plan (Records Management)
- Test the plan (at least every 6 months)
- Store the documentation off-site (MOM Policy on Automated Systems, Chapter 1-0200, Section 1-0240.00)

Is your machine plugged into a surge protector?

All electrical devices (micros, printers, modems) should be plugged into a surge protector. Surge protectors protect PC's from damage due to surges in the power supply, noise on the electrical line, and complete power loss. They do **not** protect your data. The Information Center recommends Surge Sentry surge protectors. They are available from most local computer stores and the price is approximately $100.00.

SUPPORT STRUCTURE

What is microcomputer "support"?

Microcomputer support is a system of problem determination, resolution and tracking for microcomputer users. Problem determination and resolution is vital for maintaining user productivity and satisfaction with micro systems.

Support can involve such various items as:
- telephone hot-line assistance
- on-site trouble calls
- training on hardware, software and applications
- development of applications
- installation of hardware or software
- consultation on software use or feasibilty of a new application
- acquisition assistance

How should support be provided?

Support should be provided in a knowledgable and timely manner. Those providing support should be able to solve most problems within 48 hours, or initiate problem solving with those that can solve the problem (vendors, other technical staff, etc.)

Who should provide support?

In most agencies, several levels of support should be identified. Each agency (or division, bureau, work unit, etc.) should identify a technical contact person to begin the problem determination process. If that person cannot solve the problem, he/she may have other agency resources that can assist. If there is still no resolution, agencies can "subscribe" to Information Center support services for a fixed monthly fee, based on the number of micros in the agency.

The Information Center maintains expertise on a large numnber of hardware and software products. It also conducts a bi-weekly Problem and Change meeting to discuss agency problems, share solutions, and work with major vendors (i.e. IBM, Zenith) to solve complex problems.

TRAINING POLICY

Why do agencies need a training policy?

In most agencies, employee training is necessary to properly prepare the employee for using new microcomputer technology. An employee expected to use a microcomputer on the job should be trained to use the hardware, software and applications specific to their job. Proper training can improve productivity, help agencies realize a cost benefit from their microcomputer purchases, and eliminate many of the problems associated with microcomputer use.

An agency training policy should identify the following for each employee using microcomputer equipment:

- the hardware being used
- any communications sessions that will be used
- the microcomputer software that will require proficiency
- microcomputer applications that are necessary for the job
- other identifiable microcomputer skills

How should training be provided?

Agencies have many options for providing their staff with the training they need:

- on the job training with agency experts
- computer based training -- diskette and video self-study courses
- classes at Information Services Division
- classes provided by vendors
- classes provided by private institutions: the Computer School, the Vocational Technical Center, Carroll College and others

MAINTENANCE

What should I do about maintenance?

The maintenance of microcomputers ranges from daily upkeep (cleaning, dusting, etc.) to the actual repair of microcomputers. The type of maintenance selected will in many cases be dictated by the type of equipment and the environment in which it is used. If the equipment is known to have a high failure rate or the equipment is crucial to the operation of the office, a maintenance contract is recommended.

Do you know if your machine is covered by a maintenance agreement?

Designate one person to manage PC maintenance agreements. This person should know what type of maintenance agreement you have, be able to run diagnostics, be responsible for seeing that the machine is repaired, and keep a log of all maintenance related problems.

APPENDIX A
DOCUMENTATION FORM

File Name: ________________ Creation Date: _________

DOS Version: ________ Software: __________________________

Description: ____

____

____

File Input: ____

____

____

Update Frequency: ______________________________________

Is File Critical: _____________

How Can File be Recreated? ____________________________

____

Developer: _______________________

User Responsible: _____________________

Backup User(s): _____________________ _____________________

Backup Procedures: _____________________

Security Procedures: ___________________________________

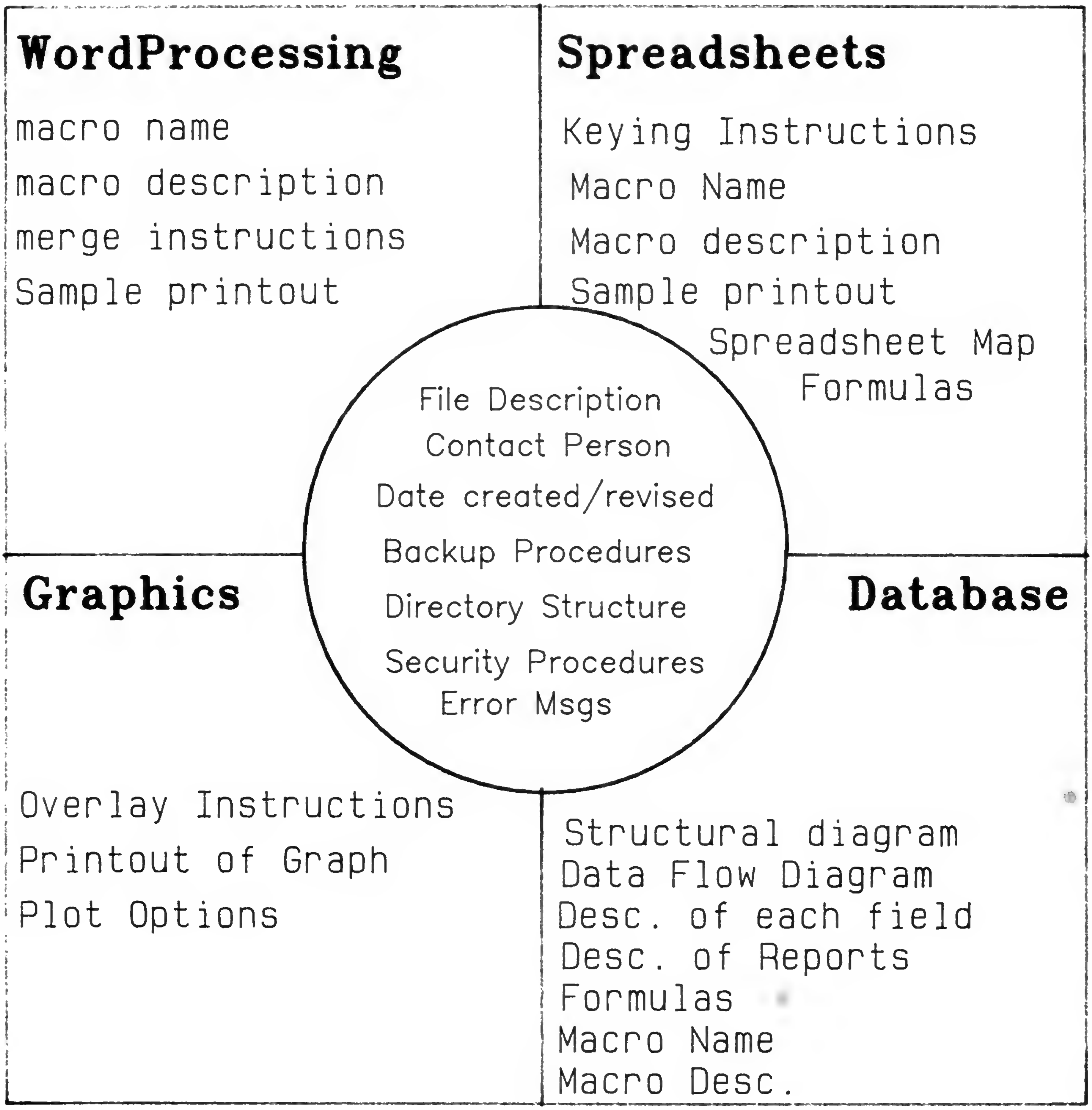
Error Messages: ____

____

Special Instructions: __________________________________

____

APPENDIX B
DOCUMENTATION CHART



WordProcessing

macro name
macro description
merge instructions
Sample printout

Spreadsheets

Keying Instructions
Macro Name
Macro description
Sample printout
Spreadsheet Map
Formulas

File Description
Contact Person
Date created/revised
Backup Procedures
Directory Structure
Security Procedures
Error Msgs

Graphics

Overlay Instructions
Printout of Graph
Plot Options

Database

Structural diagram
Data Flow Diagram
Desc. of each field
Desc. of Reports
Formulas
Macro Name
Macro Desc.

APPENDIX C
CHANGE REQUEST FORM

FROM: ______________________________

____

____

FILE NAME: ______________________________

DEVELOPER: ______________________________

DESCRIPTION OF CHANGE REQUESTED: ______________________________

____

____

____

____

____

____

____

REQUESTED IMPLEMENTATION DATE: ______________________________

ORIGINATOR'S SIGNATURE: ______________________________

PHONE: ______________________________ DATE: ______________________________

CHANGE REQUEST DISPOSITION: ______________________________

____

____

____

APPROVED: ___ DENIED: ___ DATE: ______________________________

SIGNATURE OF PERSON MAKING CHANGE: ______________________________